OPEN BANKING CREATES OPPORTUNITIES IN EBRD REGIONS

"Open banking generally refers to the ability of banking customers to authorise third parties to access their bank account data to either collect information and/or to initiate payments."

The global payments landscape has completely changed in the past decade and many countries are reviewing their regulatory approach towards payments to ensure that it serves the changing needs of customers and providers. This is happening against the backdrop of a growing e-commerce sector, the increased adoption of innovative technologies and expanding global cooperation.[1] In an attempt to accelerate the diversification of payments and offer greater choice and lower costs for consumers, countries around the world are opening up customer data and spearheading "open banking" initiatives.

1

2

1
JELENA MADIR
CHIEF COUNSEL, EBRD
(currently on leave from the EBRD)
MadirJ@ebrd.com

2
MELIS EKMEN TABOJER
DIRECTOR, INSURANCE AND FINANCIAL SERVICES, EBRD
TabojerM@ebrd.com

WHAT IS OPEN BANKING?

Open banking generally refers to the ability of banking customers to authorise third parties to access their bank account data to either collect information and/or to initiate payments.[2] In its 2019 *Future of Finance* report, the Bank of England describes open banking as "a powerful idea to give customers more control over their finances in the next decade".[3]

The United Kingdom (UK) was one of the first countries in the world to launch open banking in response to a report issued by the Competition and Markets Authority in 2016. The report highlighted a lack of competition among established, larger banks for customers' business, as well as difficulties for smaller and newer banks to compete.[4]

The open banking rules in the UK require the nine largest banks[5] to share their current account holder data through an integration technology called application programming interfaces (APIs). These APIs can then be used – with the customer's consent – by third parties, including challenger banks, Fintech companies, technology companies and credit information bureaus, to open up the financial services industry and provide consumers with products better suited to their individual needs.[6] For example, small and medium-sized enterprises could benefit from being able to compile their data from different vendors to build a comprehensive, digital business profile. They could then use their data to seek the most appropriate forms of finance at the best possible prices.[7]

Incumbent banks in the UK have been slowly but surely working on new digital services for customers. For example, HSBC was one of the first banks to release an open banking app, Connected Money, which groups customers' total spending across 30 categories, including grocery shopping and utilities.[8] Santander has partnered with the Moneybox app to offer its customers a chance to connect their accounts and round up their spare change from banking transactions into a savings account.[9] Barclays customers can also view all of their bank accounts – even the ones held with rival banks – in one app.[10]

Clearly, with greater transparency as to their customers' financial position and behaviour, traditional banks are forced to reposition their services and product offerings to match the increasing competition from multiple third-party providers and to improve the quality of customer experience. Keeping up with the fast-advancing technologies and continuous innovation, the reduction in revenues from traditional services and the increased need for cybersecurity come at a cost. And on top of it all, banks will need to convince their customers to share their financial information.

How Open Banking changes customers' relationships with banks

AISP- account information service provider | **API**- application programming interface | **FCA**- Financial Conduct Authority | **PISP**- payment initiation service provider

Source: FCA.

BALANCING THE RISKS

With open banking comes the need for increased security and structure surrounding the transfer of data between partners. This is where regulations come in, the most pertinent one being the European Union's Payment Services Directive 2 (PSD2).[11] Aiming to improve consumer protection and to make payments safer and more secure, among other things, the PSD2 introduces the requirement for strong (two-factor) customer authentication (SCA) on the majority of electronic payments and for common and secure communication. The European Banking Authority (EBA) has subsequently issued the Regulatory Technical Standards (RTS) for the SCA.[12]

One area that has been quite challenging to navigate is the interplay between the PSD2, which calls for banks to open access to customer account and transaction data, and the General Data Protection Regulation (GDPR), which requires companies, including (but not limited to) banks, to protect and handle more carefully what personal data they have, with the particular aim of giving more control to individuals over their personal information.[13]

While the European Data Protection Board has provided helpful guidance on this intersection,[14] some questions still remain. For example, the PSD2 prohibits a payment services provider (PSP) from using the personal data it has obtained for purposes other than performing the specified service. However, it is not clear how robust this prohibition may be in practice. For instance, a clever PSP may circumvent this limitation by simply broadly defining the service it offers: for example, not only account aggregation, *but also* personalised offers for other products and services. If customers were to sign up for that package and consent to such purposes, the PSP would, as a practical matter, have broadened grounds for the lawful processing of their personal data.[15]

Another challenge is the allocation of liability in case of a data breach or an unauthorised transaction. The *Future of Finance* report notes that, at least in the UK, it would be a bank, not a payment company, that may have to compensate the client for any errors or cyber-breaches before counter-suing the payment company. Obviously, this is not an optimal design.[16]

"In 2019 the EBRD, through its Legal Transition Programme, advised the National Bank of Belarus on the implementation of the new Payment Services Act."

ECONOMIES WHERE THE EBRD INVESTS

While the PSD2 has set the baseline for open banking standards, every European country can put its own flavour on it.[17] Thus, for example, in Poland, the Act of 10 May 2018, Amending the Act on Payment Services and Certain Other Acts, integrated into national law the provisions of the PSD2 and introduced a small payment institution as a new entity authorised to provide payment services.[18] The Ministry of Finance has indicated that this type of institution "may be an attractive form of running business by entities just starting to operate in the payment services market, in particular from the so-called Fintech sector".[19]

The Latvian Baltic International Bank launched an APIs sandbox solution for open banking, touted as a "safe […] environment where third-party service providers are able to test their ideas and innovations in the financial sector in general and in asset management in particular".[20]

Across the rest of the world, open banking means different things to different organisations. Still, financial industry participants around the globe are keeping a close eye on developments in the UK and Europe.[21] Whether open banking develops through UK and European-style changes or simply by the adoption of greater interoperability of APIs at the industry level, it is uniquely evolving in different parts of the world, although a common denominator is the need for security and value for the banking customer.[22]

For example, in anticipation of the rise of Fintech in Jordan, the Central Bank of Jordan has issued regulations and guidance to regulate third-party payment processors. These include the protection of e-payment users' data and personal information, the introduction of a minimum share capital for e-payment service providers and the authority for foreign companies to exercise e-payment transactions in Jordan.[23]

Turkey's largest bank, Isbank, has launched its APIs portal as it looks to work with third-party developers and Fintech companies.[24]

THE EBRD'S WORK IN BELARUS

In 2019 the EBRD, through its Legal Transition Programme, advised the National Bank of Belarus on the implementation of the new Payment Services Act, which aimed to modernise the payment services sector by transposing significant parts of the PSD2. Our recommendations focused on implementing the SCA requirements and procedures for obtaining customer consent, making payments secure, protecting customer data and using methodology to supervise PSPs by the National Bank.

In many instances the recommendations required finding a balance between being too specific and too general. With technology-related provisions in particular, specificity can encourage a standardised approach, but it can also stifle innovation and can mean that PSPs are only working with the rules to tick boxes and complete a "compliance exercise". However, where rules are too high-level, PSPs may struggle to comply with them because there is little guidance to suggest what they need to do.[25]

For example, when the EBA issued the above-described RTS, it had intentionally not specified what would be required to satisfy the elements of the SCA in order to remain technologically neutral. However, this approach led to a lot of uncertainty in the industry as to the practical implementation of systems dealing with the SCA and which methods would satisfy the authentication requirements. This confusion ultimately led the EBA to provide further guidance on each of the SCA authentication requirements.[26]

There are also further issues that have not yet been resolved by the EBA. For instance, there is some uncertainty as to whether a biometric-enabled payment card and fingerprint can authorise a contactless mobile payment, in cases where that fingerprint is also used to activate the device.[27]

To avoid this type of confusion, we recommended that the National Bank include more guidance on non-exhaustive examples on how to satisfy customer authentication. This could include setting out guidelines as to which factors are acceptable for the different authentication requirements of the SCA.

CONCLUSION

New payment services and new types of market participants are changing the way the payments and retail banking sector operate. Encouraging these new entrants is intentionally disruptive – it affects the business models, profitability, market share and consumer relationships of incumbent players – but is necessary to achieve greater innovation for the benefit of customers.[28]

However, regulators will need to take great care to balance these new disrupting forces with the need to maintain consumer protection and stability in the financial system. This will require, among other things, a well-coordinated dance with data protection regulation, which should specify how liability will be allocated in the event of a data breach and unauthorised transactions and synchronise the consent requirements with those in the regulations regarding open banking and payments. Central banks, on their end, will have to evaluate the potential risks of opening access to their services and infrastructure (such as the operation of reserve or settlement accounts) to non-bank payment providers.

1. EBRD and Hogan Lovells (2019), *Regulating Payment Services in Belarus*.
2. KPMG (2019), *Open banking opens opportunities for greater customer value*.
3. Bank of England (2019), *Future of Finance*, p. 13.
4. *Ibid.*, p. 105.
5. Barclays PLC, Lloyds Banking Group PLC, Santander, Danske, HSBC, RBS, Bank of Ireland, Nationwide and AIBG (2017). Competition and Markets Authority Retail Banking Market Investigation Order 2017.
6. Lucy Warwick-Ching (2019), *Open banking: the quiet digital revolution one year on*.
7. Bank of England (2019), *Future of Finance*, p. 61.
8. See https://www.hsbc.co.uk/connected-money/ (last accessed 13 February 2020); see also Lucy Warwick-Ching (2019), Open banking: the quiet digital revolution one year on; and https://on.ft.com/38rY23E (last accessed 13 February 2020).
9. See https://www.moneyboxapp.com/santander-launch/ (last accessed 9 January 2020); see also Lucy Warwick-Ching (January 2019), *Open banking: the quiet digital revolution one year on*.
10. See https://www.barclays.co.uk/ways-to-bank/account-aggregation/ (last accessed 9 January 2020); see also Lucy Warwick-Ching (January 2019), Open banking: the quiet digital revolution one year on.
11. Nick Ismail (2017), *Open Banking: a friend or foe to traditional banks?*
12. For a more detailed description of the SCA and the RTS, see Ben Rengard-Weinrabe and Jane Finlayson-Brown (2019), *Adapting to a Changing Payments Landscape*, in Jelena Madir (ed.), *FinTech: Law and Regulation*, Edward Elgar Publishing Ltd, UK.
13. Ross Leckow and Jess Cheng (2019), *Data laws for the digital age: How modernized legal frameworks can accelerate data-driven innovation: Challenges and opportunities*.
14. Letter from the European Data Protection Board to Sophie in't Veld (July 2018).
15. Ross Leckow and Jess Cheng (2019), *Data laws for the digital age*: *How modernized legal frameworks can accelerate data-driven innovation: Challenges and opportunities*.
16. Bank of England (2019), *Future of Finance*, p. 114.
17. Chris Thompson (2018), *Understanding the Global Evolution of Open Banking*.
18. Polish Ministry of Finance (2018), *Legal framework on payments and open banking – PSD2 implementation.2020)*.
19. *Ibid*.
20. The Paypers (2019), *Baltic International Bank implements open banking and sandbox*.
21. Chris Thompson (2018), *Understanding the Global Evolution of Open Banking*.
22. *Ibid*.
23. Clifford Chance (2019), *Fintech in the Middle East - Developments across MENA*.
24. See https://developer.isbank.com.tr/Pages/home.aspx (last accessed 9 January 2020); see also Finextra (2018), Isbank opens API portal.
25. EBRD and Hogan Lovells (2019), *Regulating Payment Services in Belarus*.
26. *Ibid*.
27. *Ibid*.
28. *Ibid*.